

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-066879

(43)Date of publication of application : 03.03.2000

(51)Int.Cl.

G06F 7/58

(21)Application number : 10-235175

(71)Applicant : NEC CORP

(22)Date of filing : 21.08.1998

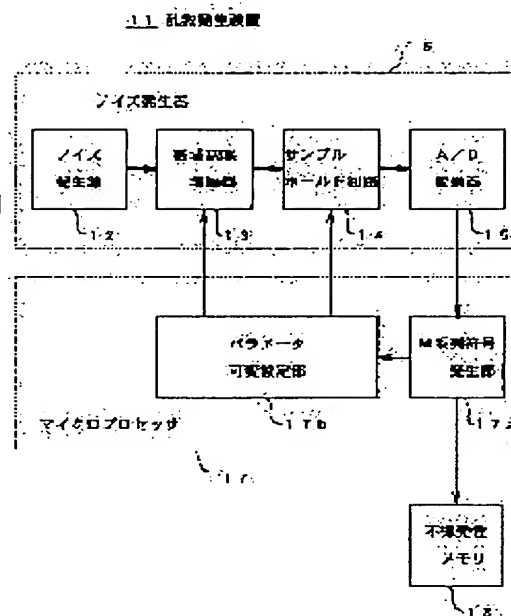
(72)Inventor : SATO YUZURU

(54) RANDOM NUMBER GENERATOR

(57)Abstract:

PROBLEM TO BE SOLVED: To generate the random number of high randomness by compounding software processing and a hardware.

SOLUTION: A noise generated by a noise generating source 12 is amplified while limiting the band through a band limit amplifier 13, further, sampled by a sample/hold circuit 14 and converted to a digital signal stream and a random number is generated by performing software processing to the provided signal stream through an M system code generating part 17a in a microprocessor 17. The trouble of simultaneously generating the same random number at two different spots is avoided and as the random number, reliability can be surely improved.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-66879
(P2000-66879A)

(43)公開日 平成12年3月3日(2000.3.3)

(51)Int.Cl.⁷

識別記号

F I

テーマコード(参考)

G 0 6 F 7/58

G 0 6 F 7/58

C

審査請求 未請求 請求項の数6 O L (全 5 頁)

(21)出願番号

特願平10-235175

(22)出願日

平成10年8月21日(1998.8.21)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 佐藤 譲

大阪府大阪市中央区城見一丁目4番24号

日本電気ホームエレクトロニクス株式会社
内

(74)代理人 100108578

弁理士 高橋 昭男 (外3名)

(54)【発明の名称】 乱数発生装置

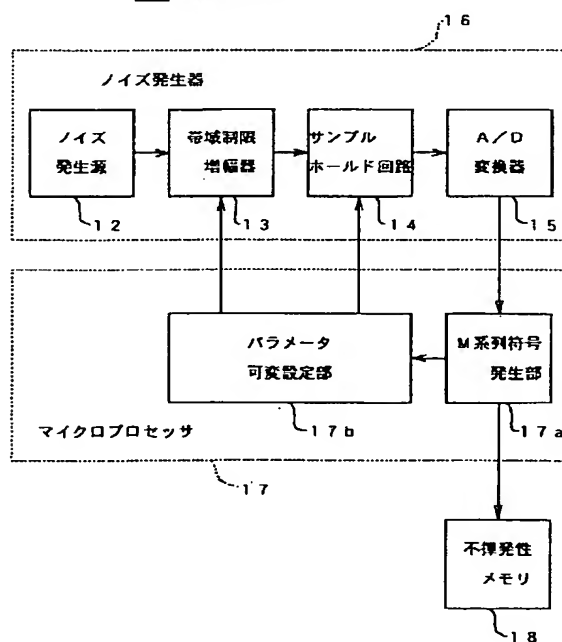
(57)【要約】

【課題】 ソフトウェア処理とハードウェアとを複合してランダム性の高い乱数を発生させる。

【解決手段】 ノイズ発生源12が発生するノイズを、帯域制限増幅器13により帯域制限して増幅し、さらにこれをサンプルホールド回路14において標本化してデジタル信号列に変換し、得られた信号列をマイクロプロセッサ17内のM系列符号発生部17aにおいてソフトウェア処理して乱数を発生する。同じ乱数が異なる二箇所で同時に発生する不都合を排除し、乱数としての信頼性を確実に高めることができる。

本発明の乱数発生装置の一実施形態を示す概略ブロック構成図

1.1 乱数発生装置



【特許請求の範囲】

【請求項 1】 ノイズを発生するノイズ発生源と、該ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、該帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をデジタル信号列に変換する A/D 変換器と、該 A/D 変換器の出力をソフトウェア処理して乱数を発生するマイクロプロセッサとを具備することを特徴とする乱数発生装置。

【請求項 2】 前記ノイズ発生源は、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生することを特徴とする請求項 1 記載の乱数発生装置。

【請求項 3】 前記マイクロプロセッサは、前記 A/D 変換器の出力を初期値としてソフトウェア処理により M 系列符号を発生することを特徴とする請求項 1 記載の乱数発生装置。

【請求項 4】 ノイズを発生するノイズ発生源と、通過帯域及び増幅度が外部から可変設定され、前記ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、標本化タイミングを外部から可変設定され、前記帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をデジタル信号列に変換する A/D 変換器と、該 A/D 変換器の出力をソフトウェア処理して乱数を発生するとともに、該乱数に基づいて前記帯域制限増幅器の通過帯域及び増幅度が又は前記サンプルホールド回路の前記標本化タイミングの少なくとも一方を可変設定するマイクロプロセッサとを具備することを特徴とする乱数発生装置。

【請求項 5】 前記ノイズ発生源は、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生することを特徴とする請求項 4 記載の乱数発生装置。

【請求項 6】 前記マイクロプロセッサは、前記 A/D 変換器の出力を初期値としてソフトウェア処理により M 系列符号を発生することを特徴とする請求項 4 記載の乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ソフトウェア処理とハードウェアとを複合してランダム性の高い乱数を発生させるようにした乱数発生装置に関する。

【0002】

【従来の技術】 高速道路の料金所において利用料金を自動的に徴収する自動料金収受システム（ETC）の導入を控え、路車間通信に必要な通信装置を搭載した車両の開発が進められている。高速道路自動料金収受システムを利用する車両は、料金所の手前の所定の通信エリア内に達した段階で、路側ビーコンを介して料金所と通信接続確立を行う必要があり、初期接続処理用として例えば 32 ビットのリンク ID を用いて通信接続確立を行う方

法が検討されている。ただし、同一の路側ビーコン通信エリア内では他の車載通信装置との通信上の衝突を避ける必要があり、このためリンク ID に非常に高いランダム性を与える乱数発生装置を開発する必要がある。

【0003】 図 2 に示す従来の乱数発生装置 1 は、乱数発生ソフトウェアを搭載したマイクロプロセッサ 2 が、初期接続処理用として 32 ビットのリンク ID を発生するものであり、ここでは乱数として M 系列符号を用いるようにしている。マイクロプロセッサ 2 は、ソフトウェア処理により M 系列符号を発生するのであるが、符号発生原理を説明しやすいよう、ここでは便宜的にハードウェア構成になぞらえてマイクロプロセッサ 2 の内部ブロックを図示してある。

【0004】 ソフトウェアが実現する M 系列符号発生手段は、0 又は 1 の状態を記憶する 1 ビットのレジスタ 3 a を 32 段に互って縦列接続したシフトレジスタ 3 と、特定段のレジスタ 3 a からデータを取り出して帰還させる帰還タップ 4 と、帰還タップ 4 からの出力を加算して初段のレジスタ 3 a に帰還する加算器（排他的論理和回路）5 とから構成され、各レジスタ 3 a が保持するビットデータは所定の動作クロックに従って順次シフトされる。なお、帰還タップ 4 の位置は特定段に設定する必要があり、こうすることで、所定周期で所定の変化形態を示す M 系列符号を発生することができる。また、初期状態として 32 段のシフトレジスタ 3 の全てのレジスタ 3 a に「0」がセットされるオール 0 の状態を避けるため、M 系列符号発生開始時に初期値として例えばオール 1 等のデータをセットするよう、初期値を保持する初期値レジスタ 6 がシフトレジスタ 3 に併設してあり、車両が路側ビーコンとの通信エリア内に進入したときに作動する起動トリガ回路 7 から供給されるトリガ信号により、初期値レジスタ 6 の保持データが初期値としてシフトレジスタ 3 に移送されるようになっている。

【0005】

【発明が解決しようとする課題】 上記従来の乱数発生装置 1 が発生する乱数の精度は、マイクロプロセッサ 2 に搭載した乱数発生ソフトウェアに依存するのは当然であるが、M 系列符号の初期値は乱数発生ソフトウェアの起動タイミングをもってセットされる。このため、起動タイミングが偶然重なってしまった 2 台の車両については、同じ初期値を用いて M 系列符号を発生する結果、同じ乱数をリンク ID として用いてしまうことがあり、通信障害を招く恐れがあった。これは、乱数発生ソフトウェアの起動タイミングが幅広く分散していないことにも一因があるが、いずれにしても M 系列符号として得られる乱数のランダム性が乏しくなるほど、他の車載通信装置との通信上の衝突を招く危険が増え、料金収受システム自体の円滑な運用の妨げとなるため、乱数のランダム性を高める対策を講じなければならないといった課題があった。

【0006】本発明は、上記課題を解決したものであり、乱数発生ソフトウェアが必要とする初期値をノイズ発生用のハードウェアから供給し、ランダム性の高い乱数を発生することを目的とするものである。

【0007】

【課題を解決するための手段】上記目的を達成するため、本発明は、ノイズを発生するノイズ発生源と、該ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、該帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をデジタル信号列に変換するA/D変換器と、該A/D変換器の出力をソフトウェア処理して乱数を発生するマイクロプロセッサとを具備することを特徴とするものである。

【0008】また、本発明は、ノイズを発生するノイズ発生源と、通過帯域及び増幅度が外部から可変設定され、前記ノイズ発生源から供給されるノイズを帯域制限して増幅する帯域制限増幅器と、標本化タイミングを外部から可変設定され、前記帯域制限増幅器の出力を標本化するサンプルホールド回路と、該サンプルホールド回路の標本化出力をデジタル信号列に変換するA/D変換器と、該A/D変換器の出力をソフトウェア処理して乱数を発生するとともに、該乱数に基づいて前記帯域制限増幅器の通過帯域及び増幅度か又は前記サンプルホールド回路の前記標本化タイミングの少なくとも一方を可変設定するマイクロプロセッサとを具備することを特徴とするものである。

【0009】

【発明の実施の形態】以下、本発明の実施形態を図1を参照して説明する。図1は、本発明の乱数発生装置の一実施形態を示す概略ブロック構成図である。

【0010】図1に示す乱数発生装置11は、ノイズ発生源12と帯域制限増幅器13とサンプルホールド回路14とA/D変換器15とを縦列接続して構成したノイズ発生器16と、乱数発生ソフトウェアを搭載したマイクロプロセッサ17と、マイクロプロセッサ17が発生した乱数を書き込む不揮発性メモリ18等から構成される。マイクロプロセッサ17は、機能的に分割集約して図示した2ブロックからなり、乱数発生ソフトウェアに従って動作するM系列符号発生部17aと、発生した乱数に応じてパラメータを可変設定するパラメータ可変設定部17bがこれらのブロックに該当する。

【0011】ノイズ発生源12は、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生する働きをするものであり、本実施形態では、例えば抵抗器の両端に発生する熱雑音を増幅してコンパレータにおいてしきい値判別することによりノイズを発生させる構成が用いられる。帯域制限増幅器13は、通過帯域及び増幅度がマイクロプロセッサ17内のパラメータ可変設定部17bにより可変設定され、ノイズ発生源12から供給される

ノイズを帯域制限して増幅する。サンプルホールド回路14は、標本化タイミングをマイクロプロセッサ17内のパラメータ可変設定部17bにより可変設定され、帯域制限増幅器13の出力を標本化する。A/D変換器15は、サンプルホールド回路14の標本化出力を量子化してデジタル信号列に変換し、マイクロプロセッサ17内のM系列符号発生部17aに初期値として与える。

【0012】ここで、ノイズ発生源12は、周期性も再現性ももたない熱雑音を発生し、これを帯域制限増幅器13を介してサンプルホールド回路14に供給する。帯域制限増幅器13の通過帯域幅と増幅度は、マイクロプロセッサ17内のパラメータ可変設定部17bが出力する通過帯域幅と増幅度を指定するパラメータにより設定されており、同様にサンプルホールド回路の標本化タイミングもまた、マイクロプロセッサ17内のパラメータ可変設定部17bが出力する標本化タイミングを指定するパラメータにより設定されている。従って、ノイズ発生源12が発生したノイズは、前回生成した乱数に応じて設定されたパラメータに従って帯域制限されかつ増幅され、続いて標本化される。

【0013】サンプルホールド回路5によって標本化されたノイズは、A/D変換器15に供給され、ここで量子化されてデジタル数値列に変換される。デジタル数値列は、マイクロプロセッサ17内のM系列符号発生部17aに初期値として供給される。M系列符号発生部17aは、A/D変換器15から供給されたデジタル数値列を初期値としてM系列符号を発生するが、ここで発生したM系列符号は乱数として不揮発性メモリ18に格納保存され、これが高速道路料金収受システムのための接続確認用リンクIDとして用いられる。また、この乱数はパラメータ可変設定部17bに供給され、次のリンクID作成時にノイズ発生器16内で必要になる通過帯域幅及び増幅度と標本化タイミングの設定に供される。

【0014】このように、上記乱数発生装置11によれば、ノイズ発生源12が発生するノイズを帯域制限して増幅し、さらにこれを標本化してデジタル信号列に変換し、得られた信号列をソフトウェア処理して乱数を発生する構成としたから、与えられた初期値に基づいて単純にソフトウェア処理によりて乱数を発生する従来装置1のように、初期値を与えるタイミングが偶然に重なってしまった場合に、同じ乱数が異なる二箇所で同時に発生するといったランダム性を損なう問題が発生することは殆どない。また、ノイズ発生源12がハードウェアに固有のランダム性をもって発生する規則性をもたないノイズにより、ソフトウェア処理に供するデジタル信号列を真のランダム性をもって発生することができ、同じ乱数が異なる二箇所で同時に発生する不都合を徹底的に排除し、発生乱数の信頼性を確実に高めることができる。

【0015】また、仮にノイズ発生源 12 自体のノイズ発生に関する非周期性が外乱による影響を受けたとしても、ノイズに由来する数値に基づいて乱数を発生するマイクロプロセッサ 17 が、この乱数に基づいてパラメータ（通過帯域幅及び増幅度と標本化タイミング）を可変設定するため、この帰還的修正とハードウェア処理との相乗効果により、きわめて高いランダム性をもって乱数を発生させることができる。

【0016】また、ノイズ発生源 12 が、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生する構成としたから、例えば抵抗器の熱雑音をコンパレータにてしきい値判別するといったハードウェア処理により安定したノイズの発生が可能であり、電氣的或いは機械的に発生した周期性や再現性をもたないノイズを用い、マイクロプロセッサ 17 によるソフトウェア処理による乱数発生を確実なものとするができる。また、マイクロプロセッサ 17 が、A/D 変換器 15 の出力を初期値としてソフトウェア処理により M 系列符号を発生するため、A/D 変換器 15 を介して与えられるノイズをもって M 系列符号の初期値を設定することで、M 系列符号が

もつランダム性を有効活用することができ、同じ乱数が異なる二箇所で同時に発生する不都合を良好に排除することができる。

【0017】なお、上記実施形態において、マイクロプロセッサ 17 が発生した乱数に応じて帯域制限増幅器 13 の通過帯域及び増幅度とサンプルホールド回路 14 の標本化タイミングの両方を可変設定する構成としたが、帯域制限増幅器 13 の通過帯域及び増幅度とサンプルホールド回路 14 の標本化タイミングのいずれか一方だけをマイクロプロセッサ 17 が発生した乱数に応じて可変設定するようにしてもよい。また、マイクロプロセッサ 17 内のパラメータ可変設定部 17b は省略することもでき、その場合は、帯域制限増幅器 13 の通過帯域及び増幅度も或いは帯域制限増幅器 13 に接続されるサンプルホールド回路 14 の標本化タイミングも固定されることになるが、ノイズ発生源 12 のランダム性に依存する乱数発生は可能である。

【0018】

【発明の効果】以上に説明したように、本発明によれば、ノイズ発生源が発生するノイズを帯域制限して増幅し、さらにこれを標本化してデジタル信号列に変換し、得られた信号列をソフトウェア処理して乱数を発生する構成としたから、与えられた初期値に基づいて単純にソフトウェア処理により乱数を発生する従来装置のように、初期値を与えるタイミングが偶然に重なってしまった場合に、同じ乱数が異なる二箇所で同時に発生するといったランダム性を損なう問題が発生することは殆どなく、ノイズ発生源がハードウェアに固有のランダム性をもって発生する規則性をもたないノイズにより、ソフ

トウェア処理に供するデジタル信号列を真のランダム性をもって発生することができ、同じ乱数が異なる二箇所で同時に発生する不都合を徹底的に排除し、発生乱数の信頼性を確実に高めることができる等の優れた効果を奏する。

【0019】また、本発明は、ノイズ発生源に接続される帯域制限増幅器の通過帯域及び増幅度か又は帯域制限増幅器に接続されるサンプルホールド回路の標本化タイミングの少なくとも一方を、マイクロプロセッサが発生乱数に従って可変設定する構成としたから、仮にノイズ発生源自体のノイズ発生に関する非周期性が外乱による影響を受けたとしても、ノイズに由来する数値に基づいて乱数を発生するマイクロプロセッサが、この乱数に基づいて通過帯域幅及び増幅度と標本化タイミングを可変設定するため、この帰還的修正とハードウェア処理との相乗効果により、きわめて高いランダム性をもって乱数を発生させることができる等の効果を奏する。

【0020】また、ノイズ発生源が、熱雑音や或いは白色雑音に相当する周期性のないノイズを発生する構成としたから、例えば抵抗器の熱雑音をコンパレータにてしきい値判別するといったハードウェア処理により安定したノイズの発生が可能であり、電氣的或いは機械的に発生した周期性や再現性をもたないノイズを用い、マイクロプロセッサによるソフトウェア処理による乱数発生を確実なものとするができる等の効果を奏する。

【0021】また、マイクロプロセッサが、A/D 変換器の出力を初期値としてソフトウェア処理により M 系列符号を発生するため、A/D 変換器を介して与えられるノイズをもって M 系列符号の初期値を設定することで、M 系列符号がもつランダム性を有効活用することができ、同じ乱数が異なる二箇所で同時に発生する不都合を良好に排除することができる等の効果を奏する。

【図面の簡単な説明】

【図 1】本発明の乱数発生装置の一実施形態を示す概略ブロック構成図である。

【図 2】従来の乱数発生装置の一例を示す概略ブロック構成図である。

【符号の説明】

- 11 乱数発生装置
- 12 ノイズ発生源
- 13 帯域制限増幅器
- 14 サンプルホールド回路
- 15 A/D 変換器
- 16 ノイズ発生器
- 17 マイクロプロセッサ
- 17a M 系列符号発生部
- 17b パラメータ可変設定部
- 18 不揮発性メモリ

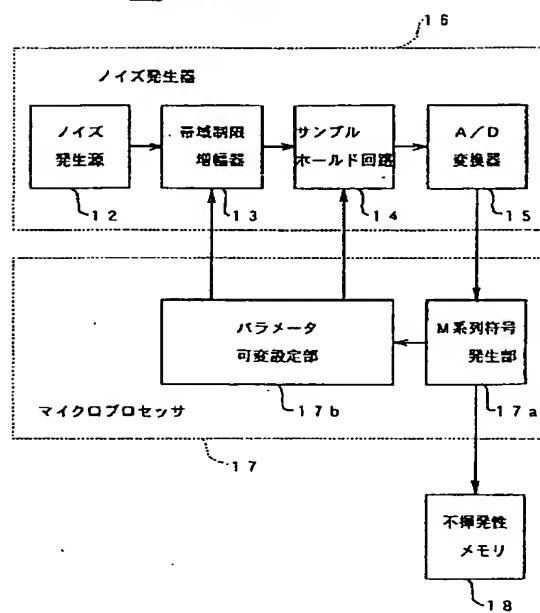
【图 1】

本発明の乱数発生装置の一実施形態を示す概略ブロック構成図

【図2】

従来の乱数発生装置の一例を示す概略ブロック構成図

1.1 乱数発生装置



1 乱散発生装置

